IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

JESUS RIVERA, *individually and on behalf of all others similarly situated,* Plaintiff, v. WEBTPA EMPLOYER SERVICES, LLC, Defendant.	Case No.: 3:24-cv-01172 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jesus Rivera (Plaintiff') bring this Class Action Complaint on behalf of himself and all others similarly situated, against Defendant WebTPA Employer Services, LLC ("WebTPA" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which are based on personal knowledge.

NATURE OF THE ACTION

1. This class action arises out of Defendant's failures to implement reasonable and industry standard data security practices to properly secure, safeguard, and adequately destroy Plaintiff's and Class Members' sensitive personal identifiable information that it had acquired and stored for its business purposes.

2. Defendant's data security failures allowed a targeted cyberattack to compromise Defendant's network (the "Data Breach") that, upon information and belief, contained personally identifiable information ("PII") of Plaintiff and other individuals ("the Class"). The Data Breach occurred between April 18, 2023, and April 23, 2023, and Defendant began sending notice letters

to Class Members on May 8, 2024.[1]

3. Defendant is a third-party administrator that provides the following services: custom health plans for self-funded employer groups; hospitals health plans; and administrative outsourcing.[2]

4. Defendant confirmed the Data Breach on March 25, 2024. Defendant posted a Notice of Data Security Incident on its website acknowledging the Data Breach.[3]

5. The PII compromised in the Data Breach included certain personal or protected health information of individuals whose PII was maintained by Defendant, including Plaintiff.

6. Upon information and belief, a wide variety of PII was implicated in the breach, including: names, dates of birth, dates of death, Social Security numbers, and contact information.

7. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' PII with which it was hired to protect.

8. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure PII from those risks left that property in a dangerous condition.

9. Upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on

[1] https://www.webtpa.com/notice (last visited 5/14/2024).
[2] *See* https://www.webtpa.com/ (last visited 5/14/2024).
[3] *See* https://www.webtpa.com/notice.

data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the PII; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

10. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' PII; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff(s) and Class Members with prompt and full notice of the Data Breach.

11. In addition, Defendant failed to properly maintain and monitor the computer network and systems that housed the PII. Had it properly monitored its property, it would have discovered the intrusion sooner rather than allowing cybercriminals a period of unimpeded access to the PII of Plaintiff and Class Members.

12. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the PII that Defendant collected and maintained is now in the hands of data thieves.

13. As a result of the Data Breach, Plaintiff and Class Members are now at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiff and Class Members must now and

for years into the future closely monitor their medical and financial accounts to guard against identity theft. As a result of Defendant's unreasonable and inadequate data security practices, Plaintiff and Class Members have suffered numerous actual and concrete injuries and damages.

14. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that the Plaintiff's and Class Members' PII was targeted, accessed, has been misused, and disseminated on the Dark Web.

15. Plaintiff and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss.

16. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their PII, consisting of an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

17. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed during the Data Breach.

18. Accordingly, Plaintiff brings this action against Defendant seeking redress for its

unlawful conduct and asserting claims for: (i) negligence and negligence *per se*, (ii) breach of third-party beneficiary contract, (iii) unjust enrichment and (iv) breach of fiduciary duty.

19. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

20. The exposure of one's PII to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiff's and the Class's PII was exactly that—private. Not anymore. Now, their PII is forever exposed and unsecure.

PARTIES

21. Plaintiff Jesus Rivera is an adult individual who at all relevant times has been a citizen and resident of Miami, Florida.

22. Defendant WebTPA Employer Services, LLC is a Texas corporation with its principal place of business at 8500 Freeport Pkwy Suite 400, Irving, TX 75063-1937. Defendant is a citizen of Texas. The registered agent for service of process is Corporation Service Company d/b/a CSC-Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Autin, Texas 78701. Upon information and belief, Defendant's customers and the victims of the Data Breach reside in multiple states.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members exceeds 100, some of whom have different

citizenship from Defendant, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

24. This Court has personal jurisdiction over Defendant because it is a Texas corporation that operates and has its principal place of business in the Dallas Division of the Northern District of Texas and conducts substantial business in this District.

25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in the Dallas Division of the Northern District of Texas. Moreover, Defendant is domiciled in this District, maintains Plaintiff's and Class Members' PII in this District, and has caused harm to Plaintiff and Class Members in this District.

FACTUAL BACKGROUND

A. Defendant Knew the Risks of Storing Valuable PII and the Foreseeable Harm to Victims.

26. At all relevant times, Defendant knew it was storing sensitive PII and that, as a result, Defendant's systems would be attractive targets for cybercriminals.

27. Defendant also knew that any breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised, as well as intrusion into their highly private health information.

28. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, Anthem, and many others.

29. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of open and anonymous

cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[4] PII, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

30. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the ITRC, in 2019, there were 1,473 reported data breaches in the United States, exposing 164 million sensitive records and 705 million "non-sensitive" records.[5]

31. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to $1.7 billion in 2018.[6]

32. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[7]

33. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[8]

---

[4] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited 2/23/2024).
[5] *Data Breach Reports: 2019 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 2, *available at* https://notified.idtheftcenter.org/s/resource#annualReportSection.
[6] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1).
[7] https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/.
[8] *Id.*

34. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's customers especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

35. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PII records can go from $20 say up to—we've even seen $60 or $70."[9] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[10]

36. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing

[9] IDExperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows: https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[10] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world*, Key findings from The Global State of Information Security® Survey 2015: https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

> custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[11]

37. The "high value of medical records on the dark web has surpassed that of social security and credit card numbers. These records can **sell for up to $1,000 online.**"[12]

38. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[13]

39. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

B. Defendant Breached its Duty to Protect its Plaintiff and Class Member's PII

40. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in

---

[11] Experian, Healthcare Data Breach: What to Know About them and What to Do After One: https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.
[12] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[13] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf.

compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA"). Under state and federal law, businesses like Defendant have duties to protect its client's current and former patients' PII/PII and to notify them about breaches.

41. The PII held by Defendant in its computer system and network included the highly sensitive PII of Plaintiff and Class Members.

42. On December 28, 2023, Defendant became aware of a ransomware attack on its system.

43. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect Plaintiff and Class Member's PII.

C. Plaintiff and Class Members Suffered Damages

44. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and Class Members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

45. Once PII or PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their

entire lives, as a result of Defendant's conduct. Further, the value of Plaintiff's and Class Members' PII has been diminished by its exposure in the Data Breach.

46. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of PII.

47. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud – this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[14]

48. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[15]

49. "Actors buying and selling PII from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[16]

50. The reality is that cybercriminals seek nefarious outcomes from a data breach" and "stolen health data can be used to carry out a variety of crimes."[17]

51. Health information in particular is likely to be used in detrimental ways—by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[18]

---

[14] https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.
[15] https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud.
[16] *Id.*
[17] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[18] *Id.*

52. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[19]

53. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[20]

54. Plaintiff and the Class members have also been injured by Defendant's unauthorized disclosure of their confidential and private medical records and PII.

55. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect Plaintiff and Class Member's PII.

COMMON INJURIES AND DAMAGES

56. As result of Defendant's ineffective and inadequate data security practices, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

57. Due to the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs

[19] https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.
[20] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/.

associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

A. The Risk of Identity Theft to Plaintiff and Class Members is Present and Ongoing

58. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

59. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

60. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

61. The dark web is an unindexed layer of the internet that requires special software or

authentication to access.[21] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[22] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

62. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at issue here.[23] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[24] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[25]

63. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of

[21] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[22] *Id.*
[23] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.
[24] *Id.; What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[25] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[26]

64. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

65. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[27]

66. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being

---

[26] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[27] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[28]

67. One such example of criminals using PII for profit is the development of "Fullz" packages. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

68. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and Class Members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

69. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[29]

70. Further, according to the same report, "rapid reporting can help law enforcement

[28] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.
[29] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

stop fraudulent transactions before a victim loses the money for good."[30] Defendant did not rapidly report to Plaintiffs and the Class that their PII had been stolen.

71. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

72. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

73. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

74. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[31]

75. The FTC has also issued numerous guidelines for businesses that highlight the

[30] *Id.*

[31] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[32]

76. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.[33]

77. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

B. Loss of Time to Mitigate the Risk of Identify Theft and Fraud

78. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn

[32] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

[33] *See, e.g.*, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices.

about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

79. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach as well as changing passwords and resecuring their own computer networks.

80. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[34] Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[35]

C. Diminution of Value of the PII

81. PII is a valuable property right.[36] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has

[34] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report").
[35] *See* https://www.identitytheft.gov/Steps.
[36] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

considerable market value.

82. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PII on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PII to adjust their insureds' medical insurance premiums.

83. PII can sell for as much as $363 per record according to the Infosec Institute.[37]

84. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[38] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[39, 40] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[41]

85. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

D. Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary

86. To date, Defendant has done little to provide Plaintiff and Class Members with

[37] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[38] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[39] https://datacoup.com/.
[40] https://digi.me/what-is-digime/.
[41] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

relief for the damages they have suffered as a result of the Data Breach, despite Plaintiff and Class Members being at risk of identity theft and fraud for the foreseeable future. Defendant has not offered any relief or protection. Furthermore, this is a tacit admission that its failure to protect their PII has caused Plaintiff and Class great injuries.[42]

87. Defendant also places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach. *Id.*

88. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

89. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

90. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

[42] *See* https://www.businesswire.com/news/home/20240206060527/en/MMRG-Notifies-Patients-of-Cybersecurity-Incident (last visited 2/26/2024).

breach, where victims can easily cancel or close credit and debit card accounts.[43] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

91. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

92. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

E. Injunctive Relief is Necessary to Protect Against Future Data Breaches

93. Moreover, Plaintiff and Class Members have an interest in ensuring that PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

94. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses and lost time. Also, he suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII is used;

b. diminution in value of their PII;

[43] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

c. compromise and continuing publication of their PII;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII; and

h. continued risk to their PII —which remains in Defendant's possession— and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII.

G. Lack of Compensation

95. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their PII in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

96. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

97. Further, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach and face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees,

credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

98. Specifically, many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

e. Addressing their inability to withdraw funds linked to compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Placing "freezes" and "alerts" with credit reporting agencies;

h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. Contacting financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

99. In addition, Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the property of loss of value damages in related cases.

100. Plaintiff and Class Members are forced to live with the anxiety that their PII — which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

101. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of PII. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, Defendant knew of the breach and has not formally notified all victims. They have yet to offer an explanation of purpose for the delay. This delay violates HIPAA and other notification requirements and increases the injuries to Plaintiff(s) and Class.

H. Plaintiff's Experience

102. Upon information and belief, Defendant obtained Plaintiff Rivera's PII in the course of its regular business operations.

103. At the time of the Data Breach—October 6, 2022 through October 16, 2022--Defendant maintained Plaintiff's PII in its system.

104. Plaintiff Rivera is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendant had he known of Defendant' lax data security policies.

105. Plaintiff Jesus Rivera received the Notice Letter, by U.S. mail, directly from Defendant, dated May 8, 2024. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his name, Social Security number, date of birth, and contact information.

106. As a result of the Data Breach, and at the direction of Defendant' Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach as well as changing passwords and resecuring his own computer network. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

107. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant' possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

108. Plaintiff additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of his PII was caused, upon information and belief, by the fact that

cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

109. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

110. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

111. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

112. Plaintiff Jesus Rivera has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant' possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

113. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following Class:

> **Nationwide Class**
> All individuals in the United States whose PII was compromised in the Data Breach reported by Defendant in May 2024 (the "Class").
>
> **Florida Subclass**
> All individuals in the State of Florida whose PII was compromised in the Data Breach reported by Defendant in May 2024 (the "Florida Subclass").

114. Excluded from the Classes is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

115. Plaintiff reserves the right to modify or amend the definition of the proposed Class and/or Florida Subclass prior to moving for class certification.

116. **Numerosity.** The class described above are so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach.

117. **Commonality.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. Whether Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had a duty to maintain the confidentiality of Plaintiff and Class Members' PII;

c. Whether Defendant breached its obligation to maintain Plaintiff and the Class members' medical information in confidence;

d. Whether Defendant was negligent in collecting, storing and safeguarding Plaintiff's and Class Members' PII, and breached its duties thereby;

e. Whether Defendant breached its fiduciary duty to Plaintiff and the Class.

f. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

g. Whether Plaintiff and Class Members are entitled to restitution or disgorgement as a result of Defendant's wrongful conduct; and

h. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

118. **Typicality**. Plaintiff's claims are typical of the claims of the Class Members. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same failure by Defendant to safeguard PII. Plaintiff and Class Members information was stored by Defendant's software, each having their PII obtained by an unauthorized third party.

119. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members he seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

120. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class Members. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its common law and statutory duties to secure PII on its network server, then Plaintiff and each Class Member suffered damages from the exposure of sensitive PII in the Data Breach.

121. **Superiority.** Given the relatively low amount recoverable by each Class Member, the expenses of individual litigation are insufficient to support or justify individual suits, making this action superior to individual actions.

122. **Manageability.** The precise size of the Class is unknown without the disclosure of Defendant's records. The claims of Plaintiff and the Class Members are substantially identical as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiff and the Class.

FIRST CAUSE OF ACTION
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

123. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

124. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

125. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

126. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing PII that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

127. Defendant's duty also arose from Defendant's position as an employer service provider. Defendant holds itself out as a trusted data collector, and thereby assumes a duty to reasonably protect its clients' customers' information. Indeed, Defendant, as a direct data collector, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

128. Defendant breached the duties owed to Plaintiff and Class Members and thus was negligent. Defendant breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to follow its own privacy policies and practices published to its clients.

129. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

130. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant or failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

131. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect the PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach involving the PII of its customers.

132. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

133. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

134. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act was intended to guard against.

135. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their PII, consisting of an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

136. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF THIRD-PARTY BENFICIARY CONTRACT
(On Behalf of Plaintiff and the Class)

137. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

138. Upon information and belief, Defendant entered into virtually identical contracts with its clients to provide software products and/or services, which included data security practices, procedures, and protocols sufficient to safeguard the PII that was to be entrusted to it.

139. Such contracts were made expressly for the benefit of Plaintiff and the Class, as it was their PII that Defendant agreed to receive and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties, and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

140. Defendant knew that if they were to breach these contracts with its clients, Plaintiff and the Class would be harmed.

141. Defendant breached its contracts with its clients and, as a result, Plaintiff and Class Members were affected by this Data Breach when Defendant failed to use reasonable data security and/or business associate monitoring measures that could have prevented the Data Breach.

142. As foreseen, Plaintiff and the Class were harmed by Defendant's failure to use reasonable data security measures to securely store and protect the files in its care, including but not limited to, the continuous and substantial risk of harm through the loss of their PII.

143. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

144. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

145. Plaintiff brings this claim in the alternative to his breach of third-party beneficiary contract claim above.

146. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their PII. In exchange, Defendant should have provided adequate data security for Plaintiff's and Class Members'.

147. Defendant knew that Plaintiff and Class Members conferred a benefit on it in the form their PII as a necessary part of their receiving healthcare services at Defendant's clients. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

148. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiff and Class Members.

149. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

150. Defendant, however, failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

151. Defendant would not be able to carry out an essential function of its regular business without the PII of Plaintiff and Class Members and derived revenue by using it for

business purposes. Plaintiff and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

152. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

153. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII, they would not have allowed their PII to be provided to Defendant.

154. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their PII.

155. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

156. Plaintiff and Class Members have no adequate remedy at law.

157. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of

benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their PII, consisting of an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

158. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

159. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

FOURTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

160. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

161. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

162. As an employee service provider, Defendant has a fiduciary relationship to its clients and their customers, like Plaintiff and the Class Members.

163. Because of that fiduciary relationship, Defendant was provided with and stored private and valuable PII related to Plaintiff and the Class, which it was required to maintain in confidence.

164. Defendant owed a fiduciary duty under common law to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

165. As a result of the parties' fiduciary relationship, Defendant had an obligation to maintain the confidentiality of the information within Plaintiff and the Class members' records.

166. Employees like Plaintiff and Class members have a privacy interest in personal information, and Defendant had a fiduciary duty not to disclose data concerning its clients' employees.

167. As a result of the parties' relationship, Defendant had possession and knowledge of confidential PII of Plaintiff and Class members, information not generally known.

168. Plaintiff and Class Members did not consent to nor authorize Defendant to release or disclose their PII to an unknown criminal actor.

169. Defendant breached the duties owed to Plaintiff and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of employee information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control the employee risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to

evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its on privacy policies and practices published to its patients; and (h) making an unauthorized and unjustified disclosure and release of Plaintiff and the Class members' PII to a criminal third party.

170. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiff and Class Members, their privacy, confidences, and PII would not have been compromised.

171. As a direct and proximate result of Defendant's breach of its fiduciary duties and breach of its confidences, Plaintiff and Class Members have suffered injuries, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their PII, consisting of an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

172. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
Violations of the Florida Deceptive and Unfair Trade Practices Act
Fla. Stat. §§ 501.201, *et seq.*
(On Behalf of Plaintiff and the Florida Subclass)

173. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein, and brings this claim on behalf of himself and the Florida Subclass (the "Class" for the purposes of this count).

174. Defendant engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Defendant obtained Plaintiff's and Class members' PII through advertising, soliciting, providing, offering, and/or distributing goods and services to its clients and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

175. As alleged herein this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

a. failure to implement adequate data security practices to safeguard PII;

b. failure to make only authorized disclosures of its clients' current and former customers' PII;

c. failure to disclose that their data security practices were inadequate to safeguard PII from theft; and

d. failure to timely and accurately disclose the Data Breach to Plaintiff and Class members.

176. Defendant's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendant engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Defendant's clients' current and former customers.

177. In committing the acts alleged above, Defendant engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately

disclosing to Defendant's clients' current and former customers that they did not follow industry best practices for the collection, use, and storage of PII.

178. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been harmed and have suffered damages including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their PII, consisting of an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

179. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff and Class members have been damaged and are entitled to recover an order providing declaratory and injunctive relief and reasonable attorneys' fees and costs, to the extent permitted by law.

180. Also as a direct result of Defendant's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiff and Class members are entitled to injunctive relief, including, but not limited to:

a. Ordering that Defendant implement measures that ensure that the PII of Defendant's clients' current and former customers is appropriately encrypted and safeguarded when stored on Defendant's network or systems;

b. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner PII not necessary for their provision of services;

c. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

d. Ordering Defendant to meaningfully educate its clients' current and former customers about the threats they face as a result of the accessibility of their PII to third parties, as well as the steps Defendant's clients' current and former customers must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grants the following:

A. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically

testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: May 16, 2024

Respectfully submitted,

/s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Telephone: 214/744-3000 / 214/744-3015 (fax)
jkendall@kendalllawgroup.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

**Pro hac vice forthcoming*
Attorneys for Plaintiff and the Proposed Class